DFS for Solaris

NFS/DFS Secure Gateway Guide and Reference

Version 3.1

GC09-3993-00

DFS for Solaris

NFS/DFS Secure Gateway Guide and Reference

Version 3.1

GC09-3993-00

Note

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 49.

First Edition (April 2000)

This edition applies to:

DFS for Solaris, Version 3.1

and to all subsequent releases and modifications until otherwise indicated in new editions.

Order publications through your IBM representative or through the IBM branch office serving your locality.

Contents

Preface

The *IBM DFS for Solaris NFS/DFS Secure Gateway Guide and Reference* contains guide and reference information about the NFS/DFS Secure Gateway for Solaris, which provides authenticated access to the DFS filespace to clients of the Network File System (NFS) by associating an NFS request with an authenticated DCE principal.

Audience

This guide and reference is intended for DFS users or administrators who need to know how to provide authenticated access to the DFS filespace for NFS clients. This book assumes that you have a working knowledge of DCE and its requirements.

Applicability

This revision applies to IBM® DFS for Solaris, Version 3.1. See your software license for details.

Purpose

The purpose of this book is to provide information about:

- Understanding the relationship of the NFS/DFS Secure Gateway to DCE and DFS
- Using the NFS/DFS Secure Gateway

Document Organization

The *IBM DFS for Solaris NFS/DFS Secure Gateway Guide and Reference* is divided into the following chapters:

- Chapter 1. Overview of the NFS/DFS Secure Gateway
- Chapter 2. Configuring Gateway Server Machines
- Chapter 3. Configuring NFS Clients to Access DFS
- Chapter 4. Accessing DFS from an NFS Client
- Chapter 5. Configuration File and Command Reference

Related Documents

For information about DCE in general, and DCE administration for Solaris in particular, refer to the following documents:

- *IBM Distributed Computing Environment for Solaris: Quick Beginnings*
- *IBM Distributed Computing Environment for AIX and Solaris: Administration Guide - Introduction*
- *IBM Distributed Computing Environment for AIX and Solaris: Administration Guide - Core Components*
- *IBM Distributed Computing Environment for AIX and Solaris: Administration Command Reference*

For information about DFS administration and commands, refer to the following documents:

- *IBM DFS for AIX and Solaris Administration Guide*
- *IBM DFS for AIX and Solaris Administration Reference*

Typographic and Keying Conventions

This guide uses the following typographic conventions:

Bold **Bold** words or characters represent system elements that you must use literally, such as commands, options, and pathnames.

Italic *Italic* words or characters represent variable values that you must supply. *Italic* type is also used to introduce a new DCE term.

`Constant width`
Examples and information that the system displays appear in `constant width` typeface.

[ ] Brackets enclose optional items in format and syntax descriptions.

{ } Braces enclose a list from which you must choose an item in format and syntax descriptions.

| A vertical bar separates items in a list of choices.

< > Angle brackets enclose the name of a key on the keyboard.

... Horizontal ellipsis points indicate that you can repeat the preceding item one or more times.

dcelocal
The OSF directory *dcelocal* in this document equates to the AIX directory */opt/dcelocal*.

This guide uses the following keying conventions:

<Ctrl- *x***> or** ^*x*

The notation **<Ctrl-** *x***>** or ^*x* followed by the name of a key indicates a control character sequence. For example, **<Ctrl-C>** means that you hold down the control key while pressing **<C>**.

<Return>

The notation **<Return>** refers to the key on your terminal or workstation that is labeled with the word Return or Enter, or with a left arrow.

Chapter 1. Overview of the NFS/DFS Secure Gateway

The Network File System (NFS) to DFS Secure Gateway provides a mechanism for granting authenticated access to the DFS filespace from an NFS client. The NFS/DFS Secure Gateway enables users to access data in the DFS filespace from a machine that is configured as an NFS client but not as a DCE client.

To use the NFS/DFS Secure Gateway for authenticated access to DFS, you must configure at least one Gateway Server machine. A Gateway Server machine must be a DFS client in the DCE cell to which access is to be provided. One function of a Gateway Server machine is to export the root of the DCE global namespace, **/...**, via NFS. Mount **/...** on each NFS client from which users are to access DFS to provide unauthenticated access to DFS.

The primary function of a Gateway Server machine is to provide DCE authentication to users of NFS clients. NFS users who have valid accounts in the registry database of the DCE cell authenticate to DCE to gain authenticated access to DFS. Depending on the needs of users and the security considerations of the DCE cell, you can provide local authentication to DCE from Gateway Server machines, remote authentication to DCE from NFS clients, or both. Local and remote authentication work as follows:

- *Local authentication* to DCE from Gateway Server machines is provided via the **dfsgw add** command. With local authentication, you can enable users to issue the **dfsgw add** command to authenticate themselves, or you can control access to DFS by allowing only system administrators to provide authentication via the **dfsgw add** command. (The **dfsgw** command suite includes additional commands to provide for central administration from Gateway Server machines.)

  Local authentication requires little configuration, but it provides a limited approach to authentication. Configuration consists only of installing the **dfsgw** commands on Gateway Server machines. However, authentication requires either administrative intervention or remote access to the Gateway Server machine (via the **telnet** program, for example); the latter approach results in user passwords being sent over the network in the clear.
- *Remote authentication* to DCE from NFS clients can be provided via the **dfs_login** command, if the command is supplied by the NFS vendor. With remote authentication, users can issue the **dfs_login** command to authenticate themselves.

  Remote authentication requires additional configuration, but it provides a less burdensome and more secure approach to authentication. Configuration consists of installing and configuring the Gateway Server (**dfsgwd**) process

on the Gateway Server machines, installing the vendor-provided **dfs_login** and **dfs_logout** commands on the NFS clients, configuring Kerberos on the NFS clients, and configuring the remote authentication service on both the Gateway Server machines and the NFS clients. However, authentication requires no administrative measures, and user passwords are never sent in the clear.

Note: The **dfs_login** and **dfs_logout** commands are not provided with DFS; these commands can be used only if they are available from your NFS vendor and have been installed on an NFS client. If these commands are not available, use the **dfsgw add** and **dfsgw delete** commands, which work in a similar fashion. See your NFS vendor documentation for the availability and use of the **dfs_login** and **dfs_logout** commands.

The **dfsgw add** and **dfs_login** commands both result in authenticated access to DFS from an NFS client. To provide a user with authenticated access, each command obtains a ticket-granting ticket (TGT) for the user from the DCE Security Service. The TGT is used to create a valid login context for the user. The login context includes a Process Activation Group (PAG), which DFS stores in the kernel of the Gateway Server machine. The PAG identifies the user's TGT; the TGT serves as the user's DCE credentials.

On the Gateway Server machine, an association is created between the UNIX user identification number (UID) of the user and the network address of the NFS client from which DFS access is desired. A mapping is then created between this pair and the PAG created for the user. The mapping is stored as an entry in a local authentication table, which, like the PAG, resides in the kernel of the machine. The mapping provides the user with authenticated access to DFS from the NFS client.

Each mapping grants a user authenticated access only from the specific NFS client for which the mapping exists. For authenticated access from a different NFS client, a user must use the **dfsgw add** or **dfs_login** command to create a new mapping for that client.

A user's DCE credentials are good only for the lifetime of the TGT. The ticket lifetime is dictated by the registry database of the DCE cell. By default, each ticket receives the default ticket lifetime in effect in the registry database. The **dfs_login** command includes a **-l** option that can be used to request a different lifetime, but a requested lifetime is constrained by the policies in effect in the registry database. A user's DCE credentials can be refreshed by using the **dfsgw add** command before the user's TGT expires. If a user's TGT expires, the user must obtain new DCE credentials. For more information on the **dfsgw add** command, see "Chapter 5. Configuration File and Command Reference" on page 25.

Before establishing a new mapping between a remote user and DCE principal, the existing mapping must be deleted. A user who wants to end an authenticated session to DFS before the credentials expire can issue either the **dfs_logout** command from the NFS client for which the credentials were granted or the **dfsgw delete** command from the Gateway Server machine. Both commands remove the user's entry for the NFS client from the authentication table on the Gateway Server machine. Either command can be used to end the authenticated session, regardless of which command was used to obtain the credentials. Because the authentication table resides in memory, all authenticated sessions are terminated if the Gateway Server is restarted.

"Chapter 2. Configuring Gateway Server Machines" on page 5 and "Chapter 3. Configuring NFS Clients to Access DFS" on page 13 provide complete instructions for configuring Gateway Server machines and NFS clients to give NFS users either local or remote authentication to DCE. "Chapter 4. Accessing DFS from an NFS Client" on page 17 provides detailed information about how users authenticate to DCE and how they access DFS from an NFS client.

Chapter 2. Configuring Gateway Server Machines

A Gateway Server machine provides authenticated access to the DFS filespace to users on NFS clients. You can configure any machine that is configured as a DFS client and an NFS server as a Gateway Server. Following successful configuration, the machine provides authenticated access to the DFS filespace, and it exports the root of the DCE namespace, **/...**, via NFS.

You can configure multiple Gateway Server machines to provide DFS access from multiple sources. However, users do not randomly select Gateway Server machines from NFS clients. By default, users on an NFS client contact the Gateway Server machine that exports **/...** to the client. If you want to balance the load among multiple Gateway Servers, you must configure your NFS clients so that each client mounts **/...** on a particular Gateway Server machine. (See "Chapter 3. Configuring NFS Clients to Access DFS" on page 13 for information on configuring NFS clients.)

Depending on how closely you want to control access to the DFS filespace, configure your Gateway Server machines in one of the following ways:

- Configure the Gateway Server machines so that users *cannot* issue the **dfs_login** command to authenticate to DCE.

  This configuration allows system administrators to manage all DCE authentication from the Gateway Server machines. You can allow users to issue the **dfsgw add** command themselves, or you can limit use of the command to administrators only. To configure a Gateway Server machine without enabling remote authentication via the **dfs_login** command, follow the instructions in "Configuring a Gateway Server Without Enabling Remote Authentication" on page 6.
- Configure the Gateway Server machines so that users *can* issue the **dfs_login** command to remotely authenticate to DCE.

  This configuration allows users of NFS clients to acquire their own DCE credentials from the NFS clients. To configure a Gateway Server machine and enable remote authentication via the **dfs_login** command, follow the instructions in "Configuring a Gateway Server and Enabling Remote Authentication" on page 7.

Note: The **dfs_login** and **dfs_logout** commands are not provided with DFS; these commands can be used only if they are available from your NFS vendor and have been installed on an NFS client. If these commands are not available, use the **dfsgw add** and **dfsgw delete** commands, which work in a similar fashion. See your NFS vendor documentation for the availability and use of the **dfs_login** and **dfs_logout** commands.

Before configuring a Gateway Server machine, you must do the following:

- Configure a DCE cell that includes DFS.
- Configure each machine that is to become a Gateway Server as a DFS client and an NFS server.
- Ensure proper synchronization among the system clocks on machines that are to become Gateway Servers, machines configured as NFS clients that are to contact the Gateway Servers, and machines in the DCE cell to be contacted. You must keep the system clocks on these machines synchronized at all times.

Configuring a Gateway Server Without Enabling Remote Authentication

Perform the steps in this section to enable DCE authentication from a Gateway Server machine without enabling it from NFS clients that contact the Gateway Server. Users can authenticate only by issuing the **dfsgw add** command on the Gateway Server machine (or by having a system administrator issue the command for them).

1. Log in as the local superuser **root** on the machine.
2. Install the binary file for the **dfsgw** command suite in the directory *dcelocal*/**bin** on the machine. The **dfsgw** command suite provides a local interface to the authentication table maintained on the Gateway Server machine. Commands in the **dfsgw** suite can be used to add, delete, and view mappings in the authentication table. (See "Authenticating to DCE from a Gateway Server Machine" on page 21, "Determining Whether a Specific User Is Authenticated to DCE" on page 22, and "Displaying Information About All Users Who Are Authenticated to DCE" on page 22 for information about using these commands.)
3. Export the DCE global root directory, **/...**, via NFS. This is typically accomplished via the **share** command; the exact command and procedure depends on your vendor's implementation of NFS, as detailed in the vendor documentation.

The Gateway Server machine is now configured to provide DCE authentication only via the **dfsgw add** command. Repeat these steps on each DFS client that is to be configured as a Gateway Server in this manner. If you later decide to allow users to authenticate to DCE from NFS clients that contact the Gateway Server, simply perform the steps in "Configuring a Gateway Server and Enabling Remote Authentication" on page 7 on the Gateway Server machine.

Configuring a Gateway Server and Enabling Remote Authentication

Perform the steps in this section to enable DCE authentication either from a Gateway Server machine or from NFS clients that contact the Gateway Server. Users authenticate from the Gateway Server machine by issuing the **dfsgw add** command; they authenticate from an NFS client by issuing the **dfs_login** command. A Gateway Server machine to be configured in this manner runs the Gateway Server process (**dfsgwd**). The steps in "Configuring the Gateway Server Process" on page 9 configure the **dfsgwd** process on the Gateway Server machine.

It is recommended that a Gateway Server machine configured in this way also runs the Basic OverSeer (BOS) Server to monitor and simplify administration of the **dfsgwd** process. The steps in "Configuring the BOS Server Process" configure a BOS Server process (**bosserver**) on the Gateway Server machine. Perform the steps in "Configuring the BOS Server Process" only if the BOS Server is not already running on the machine. (Note that you typically run the BOS Server only on DFS servers, but you can run it on DFS clients. See the *IBM DFS for AIX and Solaris Administration Guide* for more information about the BOS Server.)

Configuring the BOS Server Process

To configure the BOS Server process (**bosserver**), perform the following steps on the machine to be configured as a Gateway Server. In all cases, *hostname* is the hostname of the local machine. (Note that it can be necessary to install the **bosserver** binary file on the machine if it is not already present.)

1. Authenticate to DCE as a principal who has the following ACL permissions on entries in the registry database:
   - The **i** permission on the directory **hosts/***hostname*.
   - The **m**, **a**, **u**, **g**, and **c** permissions on the principal **hosts/***hostname***/dfs-server**. The principal is created during the configuration steps.
   - The **t** and **M** permissions on the group **subsys/dce/dfs-admin**.
   - The **R**, **t**, and **M** permissions on the organization **none**.
   - The **r** permission on the registry Policy object for the DCE cell.

     This requirement is most easily met by authenticating to a privileged DCE identity (for example, **cell_admin** or a principal who is a member of the group **acct-admin**).
2. Create the principal **hosts/***hostname***/dfs-server**, and create an account for the principal. In the commands, *password* is the password of the DCE identity to which you are authenticated.

```
$ dcecp
dcecp> principal create hosts/hostname/dfs-server
dcecp> account create hosts/hostname/dfs-server -group subsys/dce/dfs-admin
-org none -password password mypwd password
```

3. Grant the group **subsys/dce/dfs-admin** the appropriate permissions on the ACL for the **hosts/***hostname*/**dfs-server** principal in the registry database:

   ```
   dcecp> acl mod /.:/sec/principal/hosts/hostname/dfs-server
   -add {group subsys/dce/dfs-admin rcDnfmag}
   dcecp> exit
   ```

4. Use the **su** command to become the local superuser **root** on the machine:

   ```
   $ su
   Password: root_password
   ```

5. Add a server key for the **hosts/***hostname*/**dfs-server** principal to the **/krb5/v5srvtab** keytab file on the machine. The **dced** process recognizes the keytab file by the entry name **self**. The command creates the keytab file if the file does not already exist. In the commands, *password* is the password of the DCE identity to which you were authenticated when you created the principal.

   ```
   # dcecp
   dcecp> keytab add self -member hosts/hostname/dfs-server -key password
   dcecp> keytab add self -member hosts/hostname/dfs-server -random -registry
   dcecp> exit
   ```

6. Remove the **BosConfig** file and any administrative lists that possibly exist from a previous configuration of the BOS Server on the machine:

   ```
   # rm -f dcelocal/var/dfs/BosConfig
   # rm -f dcelocal/var/dfs/admin.*
   ```

7. Start the **bosserver** process with DFS authorization checking disabled. The process creates a new **BosConfig** file and a new **admin.bos** file, which is the administrative list for the BOS Server.

   ```
   # dcelocal/bin/bosserver -noauth &
   ```

8. Add the group **subsys/dce/dfs-admin** to the **admin.bos** file:

   ```
   # dcelocal/bin/bos addadmin -server /.:/hosts/hostname -adminlist admin.bos
   -group subsys/dce/dfs-admin
   ```

9. Enable DFS authorization checking by the BOS Server:

   ```
   # dcelocal/bin/bos setauth -server /.:/hosts/hostname -authchecking on
   ```

10. Configure the **bosserver** process to start automatically when the system is restarted by removing the two number signs (**#**) from the following line of the **/etc/rc.dfs** file (or its equivalent):

    ```
    ##daemonrunning $DCELOCAL/bin/bosserver
    ```

The BOS Server is now fully configured on the machine.

Configuring the Gateway Server Process

To configure the Gateway Server (**dfsgwd**) process, perform the following steps on the machine to be configured as a Gateway Server. The steps assume that the BOS Server is already running on the machine. In all of the steps, *hostname* is the hostname of the local machine.

Note: You need to perform some steps only when you configure the first Gateway Server process. Such steps are qualified with the phrase *for the first Gateway Server process*.

1. If you have not already done so, perform all the steps in "Configuring a Gateway Server Without Enabling Remote Authentication" on page 6 to install the **dfsgw** binary file on the machine and to export **/...** from the machine.
2. If you have not already done so, log in as the local superuser **root** on the machine.
3. Install the binary file for the **dfsgwd** process in the directory *dcelocal*/**bin** on the machine. The **dfsgwd** process provides users of NFS clients with a remote interface to the authentication table maintained on the Gateway Server machine.
4. Add the **dfsgw** service to the Internet services database. The **dfsgw** service provides the login facility for the NFS/DFS Secure Gateway. To add the service, do one of the following:
   - If you use the **/etc/services** file in your environment, add an entry for the **dfsgw** service to the **/etc/services** file on the machine.
   - If you use a Network Information Service (NIS) services map in your environment, add an entry for the **dfsgw** service to the NIS services map file on the NIS master. Add the entry to the services map only *for the first Gateway Server process*; do not add the entry for additional Gateway Server processes or NFS clients.

   In either case, you need to add the following entry for the service:

   ```
   dfsgw     438/udp     dlog
   ```

   where **dfsgw** is the name of the service, **438** is the port at which the service receives RPCs, **udp** is the protocol the service uses to communicate, and **dlog** is an alias for the **dfsgw** service.
5. Authenticate to DCE as a principal who has the following ACL permissions on entries in the registry database:
   - The **i** permission on the directory **hosts/***hostname*.
   - *For the first Gateway Server process*, the **i** permission on the directory **subsys/dce**.

- The **m**, **a**, **u**, and **g** permissions on the principal **hosts/***hostname***dfsgw-server**. The principal is created during the configuration steps.
- The **t** and **M** permissions on the group **subsys/dce/dfsgw-admin**. The group is created during the configuration steps.
- The **R**, **t**, and **M** permissions on the organization **none**.
- The **r** permission on the registry Policy object for the DCE cell.

This requirement is most easily met by authenticating to a privileged DCE identity (for example, **cell_admin** or a principal who is a member of the group **acct-admin**).

6. Invoke the **dcecp** command:

   ```
   $ dcecp
   ```

7. *For the first Gateway Server process*, create the group **subsys/dce/dfsgw-admin** in the registry database. Use the following **dcecp** command to create the group:

   ```
   dcecp> group create subsys/dce/dfsgw-admin
   ```

8. Create the principal **hosts/***hostname***/dfsgw-server**, and create an account for the principal. The Gateway Server process communicates as the principal **hosts/***hostname***/dfsgw-server**. In the commands, *password* is the password of the DCE identity to which you are authenticated.

   ```
   dcecp> principal create hosts/hostname/dfsgw-server
   dcecp> account create hosts/hostname/dfsgw-server -group subsys/dce/dfsgw-admin
   -org none -password password -mypwd password
   dcecp> exit
   ```

9. Use the **su** command to become the local superuser **root** on the machine:

   ```
   $ su
   Password: root_password
   ```

10. Add a server key for the **hosts/***hostname***/dfsgw-server** principal to the **krb5/v5srvtab** keytab file on the machine. The **dced** process recognizes the keytab file by the entry name **self**. In the commands, *password* is the password of the DCE identity to which you were authenticated when you created the principal.

    ```
    # dcecp
    dcecp> keytab add self -member hosts/hostname/dfsgw-server -key password
    dcecp> keytab add self -member hosts/hostname/dfsgw-server -random -registry
    dcecp> exit
    ```

11. Log out as the local superuser **root** to return to your authenticated DCE identity.

12. If your current DCE identity is not included in the *dcelocal***/var/dfs/admin.bos** file on the machine, either add the identity to the file or authenticate to DCE as a principal that is included in the file. You can use the **bos lsadmin** command to list the principals and groups included in the **admin.bos** file:

    ```
    $ dcelocal/bin/bos lsadmin -server /.:/hosts/hostname -adminlist admin.bos
    ```

13. Create a **simple** BOS Server process named **dfsgw** to run the **dfsgwd** server process:

    $ *dcelocal*/**bin/bos create -server /.:/hosts/***hostname* **-process dfsgw -type simple -cmd** *dcelocal*/**bin/dfsgwd**

The Gateway Server process is now fully configured on the machine.

Chapter 3. Configuring NFS Clients to Access DFS

After you have configured at least one Gateway Server machine according to the instructions in “Chapter 2. Configuring Gateway Server Machines” on page 5, you can configure your NFS clients to provide access to the DFS filespace. Users who have DCE accounts can then authenticate to DCE for authenticated access to DFS from the NFS clients. Authenticating to DCE provides these users with the privileges and permissions associated with their DCE identities.

Configure each NFS client that is to provide access to DFS in one of the following ways, depending on how you configured your Gateway Server machines:

- If you configured your Gateway Servers so that users *cannot* issue the **dfs_login** command to authenticate to DCE (configured your NFS clients without enabling DCE authentication via the **dfs_login** command), follow the instructions in “Configuring a Client Without Enabling Remote Authentication” on page 14.
- If you configured your Gateway Servers so that users *can* issue the **dfs_login** command to authenticate to DCE (configured your NFS clients and enable DCE authentication via the **dfs_login** command), follow the instructions in “Configuring a Client and Enabling Remote Authentication” on page 14.

Note: The **dfs_login** and **dfs_logout** commands are not provided with DFS; these commands can be used only if they are available from your NFS vendor and have been installed on an NFS client. If these commands are not available, use the **dfsgw add** and **dfsgw delete** commands, which work in a similar fashion. See your NFS vendor documentation for the availability and use of the **dfs_login** and **dfs_logout** commands.

Because the steps in each of these sections mount **/...** on an NFS client, users who do not have DCE accounts can still use the NFS client for unauthenticated access; see “Authenticated Access to DFS” on page 18 for more information about authenticated access.)

Configuring a Client Without Enabling Remote Authentication

If you configured your Gateway Server machines so that users cannot issue the **dfs_login** command to authenticate to DCE, perform the steps in this section to configure your NFS clients. The steps enable DFS access from an NFS client without enabling DCE authentication from the client. Users can authenticate only via the **dfsgw add** command.

1. Log in as the local superuser **root** on the machine.
2. Mount the root of the DCE namespace, **/...**, on the machine. In the command, *hostname* is the hostname of a Gateway Server machine which exports **/...**. Each Gateway Server machine configured as a Gateway Server exports **/...**. To achieve proper load balancing if you configure multiple Gateway Server machines, ensure that the mounts of **/...** on your NFS clients are divided evenly among your Gateway Servers. (You can use the NFS automount mechanism with a direct automount map to mount **/...**; see your vendor's NFS documentation for more information.)

   ```
   # mkdir /...
   # mount hostname:/... /...
   ```
3. Create a symbolic link from **/:** to the root of the DFS filespace for the host DCE cell, **/.../***cellname*/**fs**. In the command, *cellname* is the name of the DCE cell to be accessed from the NFS client (the cell in which the machine that exports **/...** is configured as a DFS client).

   ```
   # ln -s /.../cellname/fs /:
   ```
4. Verify that the NFS mount of DCE was successful by using the **ls** command to list the contents of **/:**, which leads to the root directory of the DFS filespace. The command yields the same output from the NFS client that it does from a DFS client of the DCE cell.

   ```
   # ls /:
   ```

The NFS client is now configured to provide access to DFS but not to allow users of the client to authenticate to DCE with the **dfs_login** command. Repeat these steps on each NFS client to be configured in this manner. If you later decide to allow users to authenticate to DCE from the NFS client, simply perform the steps in "Configuring a Client and Enabling Remote Authentication" on the client.

Configuring a Client and Enabling Remote Authentication

If you configured your Gateway Server machines so that users can issue the **dfs_login** command to authenticate to DCE, perform the steps in this section to configure your NFS clients. The steps enable both DFS and DCE authentication from an NFS client. Users can authenticate via either the **dfsgw add** command or the **dfs_login** command.

Note: The **dfs_login** and **dfs_logout** commands are not provided with DFS; these commands can be used only if they are available from your NFS vendor. If these commands are not available, use the **dfsgw add** and **dfsgw delete** commands, which work in a similar fashion. See your NFS vendor documentation for the availability and use of the **dfs_login** and **dfs_logout** commands.

1. If you have not already done so, perform all of the steps in "Configuring a Client Without Enabling Remote Authentication" on page 14 to mount **/...** on the machine.
2. If you have not already done so, log in as the local superuser **root** on the machine.
3. Install the binary files for the **dfs_login** and **dfs_logout** commands in the **/usr/bin** directory on the machine. These commands provide the following functionality:

   dfs_login
   Establishes an authenticated session for users of the NFS client by obtaining DCE credentials on a Gateway Server machine. (See "Authenticating to DCE from an NFS Client" on page 19 for information about using this command.)

   dfs_logout
   Ends an authenticated session established with the **dfs_login** command. (See "Authenticating to DCE from an NFS Client" on page 19 for information about using this command.)

   (The **dfs_login** and **dfs_logout** commands use version 5 of Kerberos to communicate with the DCE Security Service.)
4. Create the Kerberos configuration file named **/krb5/krb.conf**. The **dfs_login** command reads this file to determine the name of a DCE Security Server that it can contact. This file must be identical to the **/krb5/krb.conf** file on machines in the host DCE cell; copy it from a machine in the DCE cell.
5. Create the Kerberos configuration file named **/krb5/krb.realms**. The Kerberos runtime uses the information in this file to translate Internet domains to the corresponding Kerberos realms. In the file, the Kerberos realm has the same name as the DCE cell. Each line of the file must have the following format:

   ```
   domain   krb-realm
   ```

   where *domain* is the name of the local Internet domain, and *krb-realm* is the name of the Kerberos realm (the name of the DCE cell to be accessed). For example, in the following **krb.realms** file, **def.com** is the name of the Internet domain, and **abc.com** is the name of the DCE cell. If machines from multiple domains are to contact the DCE cell, you need a separate line for each domain. Note that realm names are case-sensitive.

```
.DEF.COM   abc.com
```

6. If you use the **/etc/services** file in your environment, add the following entry for the **dfsgw** service to the **/etc/services** file on the machine:

   ```
   dfsgw      438/udp      dlog
   ```

   where **dfsgw** is the name of the service, **438** is the port at which the service receives RPCs, **udp** is the protocol the service uses to communicate, and **dlog** is an alias for the **dfsgw** service.

   If you use an NIS services map in your environment, you added an entry to the services map file when you configured the first Gateway Server process. You do *not* need to add the entry to the services map when you configure NFS clients.

The NFS client is now configured to provide access to DFS and to allow users of the client to authenticate to DCE with the **dfs_login** command. Repeat these steps on each NFS client to be configured in this manner.

Chapter 4. Accessing DFS from an NFS Client

After a Gateway Server machine and one or more NFS clients are configured according to the instructions in "Chapter 2. Configuring Gateway Server Machines" on page 5 and "Chapter 3. Configuring NFS Clients to Access DFS" on page 13, users of the NFS clients can access data in the DFS filespace. Users can access files and directories in DFS by full **/.../***cellname*/**fs** pathnames or by abbreviated pathnames that use the **/:** link to the DFS filespace. The following are equivalent pathnames for the file **myfile** in the DFS filespace of the DCE cell **abc.com**:

```
/.../abc.com/fs/myfile
/:/myfile
```

All users have unauthenticated access to DFS. Users who have DCE accounts can authenticate to their DCE identities for authenticated access to DFS. The following subsections provide more information about these two types of access.

When accessing DFS data from a DFS client, the DFS Cache Manager caches local copies of files accessed from File Server machines. When accessing DFS data from an NFS client, NFS background I/O daemons cache local copies of files accessed via the NFS server. The caching of information by the NFS daemons can affect how quickly changes you make to data in DFS become visible to other users.

Unauthenticated Access to DFS

Unauthenticated access is provided to users who access DFS without first authenticating to DCE. For a user who does not have an account in the DCE registry database, unauthenticated access is the only available form of access. Unauthenticated access requires no preliminary steps; users simply access data in DFS from an NFS client.

Unauthenticated users receive the following permissions for objects (files and directories) in the DFS filespace:

- For objects in non-LFS filesets, unauthenticated users receive the permissions granted by the **other** mode bits of the object.
- For objects in DCE LFS filesets, unauthenticated users receive the permissions granted by the **any_other** entry, if it exists, on the ACL of the object. The **mask_obj** entry filters permissions granted via the **any_other** entry.

When an unauthenticated user creates an object, the object is owned by the user **nobody** and the group **nogroup**. The UID of the user **nobody** is **-2**, and the GID of the group **nogroup** is also **-2**. (Identities and ID numbers of an unauthenticated user and group can vary between systems; see your vendor's documentation for more information.)

Unauthenticated access is provided with the NFS/DFS Secure Gateway as a side effect of configuring Gateway Server machines and NFS clients. Unauthenticated access is available without the NFS/DFS Secure Gateway. Simply export **/...** from a DFS client that is also an NFS Server, and mount **/...** on each NFS client from which users are to access DFS.

Authenticated Access to DFS

Authenticated access is available to users who have accounts in the DCE cell. When an authenticated user accesses an object in the DFS filespace, the user receives the permissions associated with the DCE identity. When the user creates an object, the object is owned by the DCE principal and its primary group.

To authenticate to DCE, you can issue either of the following commands, both of which establish credentials recognized by the DCE Security Service:

- From an NFS client, issue the **dfs_login** command. (See "Authenticating to DCE from an NFS Client" on page 19 for more information.)
- From a Gateway Server machine, issue the **dfsgw add** command. (See "Authenticating to DCE from a Gateway Server Machine" on page 21 for more information.)

Note: The **dfs_login** and **dfs_logout** commands are not provided with DFS; these commands can be used only if they are available from your NFS vendor and have been installed on an NFS client. If these commands are not available, use the **dfsgw add** and **dfsgw delete** commands, which work in a similar fashion. See your NFS vendor documentation for the availability and use of the **dfs_login** and **dfs_logout** commands.

A user who desires authenticated access to DFS must have a principal and account in the registry database of the DCE cell. An entry must exist for the user in the **/etc/passwd** file on the machine configured as a Gateway Server and on each NFS client from which the user is to access DCE. It is recommended that the user's UID in the **/etc/passwd** file match the user's UID in the DCE registry database. (On a DCE client, the **passwd_export** command can be used to keep **/etc/passwd** files current with respect to the registry database; see the *IBM Distributed Computing Environment for AIX and Solaris: Administration Guide - Core Components* for more information.)

The **dfsgw add** command can be used to refresh DCE credentials. If they are not refreshed, DCE credentials (tickets) expire after the lifetime specified by the DCE Security Service. After they expire, the tickets can no longer be used for authenticated access. To end an authenticated session before the ticket lifetime has passed, you can issue either of the following commands:

- From the NFS client from which authenticated access to DFS is provided, enter the **dfs_logout** command. (See "Authenticating to DCE from an NFS Client")
- From the Gateway Server machine via which the DFS is accessed, enter the **dfsgw delete** command. (See "Authenticating to DCE from a Gateway Server Machine" on page 21)

Both commands remove the entry from the authentication table that provides authenticated access from the NFS client. Regardless of which command you used to establish the DCE credentials (**dfs_login** or **dfsgw add**), you can end the authenticated session with the **dfs_logout** command or the **dfsgw delete** command. Neither command affects authenticated access from the other NFS clients. If your DCE credentials are the basis of another entry in the authentication table, you still have authenticated access via that other entry.

To refresh your DCE credentials before they expire, use the **dfsgw add** command, which refreshes the ticket lifetime of your existing TGT. to obtain new credentials, then use the **dfs_login** or **dfsgw add** command to replace your existing TGT with the new TGT.

Note that if you configure multiple Gateway Server machines, each server machine houses its own authentication table. The **dfs_login** and **dfs_logout** commands affect entries only in the authentication table maintained on the Gateway Server machine they contact; commands in the **dfsgw** suite affect entries only in the authentication table on the machine on which they are issued.

Authenticating to DCE from an NFS Client

The **dfs_login** command authenticates a user to DCE from an NFS client. The command contacts the DCE Security Service to obtain a TGT and a service ticket for the Gateway Server (**dfsgwd**) process for the user. It encrypts the user's TGT with the service ticket and sends these to the Gateway Server process. It also sends the UID of the user who issues the command and the network address of the NFS client from which the command is issued. The Gateway Server process uses this information to create a valid login context, including a PAG, and an entry in the authentication table for the user.

Note: The **dfs_login** and **dfs_logout** commands are not provided with DFS; these commands are provided by your NFS vendor. The instructions

given for the **dfs_login** and **dfs_logout** commands can only be performed if your NFS vendor provides these commands. If these commands are not available, use the instructions for the **dfsgw add** and **dfsgw delete** commands, which work in a similar fashion. See your NFS vendor documentation for the availability and use of the **dfs_login** and **dfs_logout** commands.

The syntax of the **dfs_login** command follows:

dfs_login [**-h** *hostname*] [**-l** *hh[:mm]*] [*dce_principal*] [*dce_password*]

where:

-h *hostname*
: Specifies the hostname of the Gateway Server machine. By default, the command uses the hostname of the machine that exports **/...** to the NFS client. Use this option to contact a different Gateway Server.

-l *hh[:mm]*
: Specifies the lifetime to assign to the service ticket obtained with the command. Enter the lifetime as a number of hours and, optionally, minutes. A value specified with this option is subject to the policies in effect in the registry database of the DCE cell. By default, the ticket is assigned the DCE cell's default lifetime.

dce_principal
: Specifies the DCE principal name of the user for whom to obtain a ticket. By default, the command uses the name of the issuer of the command.

dce_password
: Provides the DCE password of the specified user. If you do not specify a password, the command prompts for a password if one of the following is true: You name a user other than yourself; you name yourself and you do not already have a valid TGT; or you do not name a user and you do not already have a valid TGT. The command does not prompt for a password if you do not name a different user and you already have a valid TGT.

For example, the user named **ludwig** issues the following **dfs_login** command to authenticate to DCE from an NFS client:

```
$ dfs_login
Password for ludwig@abc.com: password
```

where *password* is the DCE password of the user **ludwig**. In the example, the user **ludwig** does not already have a valid TGT, so the command prompts for the user's password and obtains a TGT for the user. If the login succeeds, the **dfs_login** command returns no messages.

To end the authenticated session before the DCE credentials expire, issue the **dfs_logout** command from the NFS client. The command removes the user's entry from the authentication table on the Gateway Server machine. The command can be issued either by the user whose entry is to be removed from the authentication table or by a user who is logged into the NFS client as the local superuser **root**. The command has no effect on authenticated access that the user has established with other NFS clients.

The syntax of the **dfs_logout** command follows:

dfs_logout [**-h** *hostname*] [*dce_principal*]

where:

-h *hostname*
: Specifies the hostname of the Gateway Server machine. By default, the command uses the hostname of the machine that exports **/...** to the NFS client. Use this option to contact a different Gateway Server.

dce_principal
: Specifies the DCE principal name of the user whose entry is to be removed from the authentication table. By default, the command deletes the entry for the user who issues the command.

For example, the following ends the authenticated session of the issuer of the command:

```
$ dfs_logout
```

Authenticating to DCE from a Gateway Server Machine

The **dfsgw add** command authenticates a user to DCE from a Gateway Server machine. Users can use the **dfsgw add** command if the **dfs_login** command is not installed on the NFS client from which they desire access to DFS. System administrators can use the command to administer authenticated access to DFS from a Gateway Server machine. Note that for NFS clients not configured to enable DCE authentication, the **dfsgw add** command represents the only way to authenticate with DCE.

The **dfsgw add** command provides essentially the same functionality as the **dfs_login** command. However, unlike the **dfs_login** command, the **dfsgw add** command does not communicate with the Gateway Server (**dfsgwd**) process; it creates the login context and entry in the authentication table. In addition, it requires the issuer to identify the user for whom authenticated access is desired and the NFS client from which the user is to access DFS. Also, the **dfs_login** command allows the issuer to request a ticket lifetime.

To end a user's authenticated session from a specified NFS client, issue the **dfsgw delete** command on the Gateway Server machine. The command

provides the same functionality from a Gateway Server machine that the **dfs_logout** command provides from an NFS client. The **dfsgw delete** command can be issued either by the user whose entry is to be removed from the authentication table or by a user who is logged into the Gateway Server machine as the local superuser **root**. The command has no effect on authenticated sessions the user has with other NFS clients.

For detailed information about the use and syntax of the **dfsgw add** and **dfsgw delete** commands, see the reference pages in the "Chapter 5. Configuration File and Command Reference" on page 25.

Determining Whether a Specific User Is Authenticated to DCE

The **dfsgw query** command determines whether a specific user is authenticated to DCE via the Gateway Server machine. The command can be issued either by the user whose authentication is to be determined or by a user who is logged in as the local superuser **root** on the machine configured as a Gateway Server.

The command looks for an entry for the user in the authentication table on the Gateway Server machine on which it is issued. If your environment includes multiple Gateway Server machines, you must issue the command on the Gateway Server machine whose authentication table is to be examined. The command displays information about a user's entry regardless of whether the user authenticated via the **dfs_login** command or the **dfsgw add** command.

See the reference page for the **dfsgw query** command for more information about the command.

Displaying Information About All Users Who Are Authenticated to DCE

The **dfsgw list** command lists all users who are authenticated to DCE via the Gateway Server machine. The command lists all entries in the authentication table on the Gateway Server machine on which it is issued. If your environment includes multiple Gateway Server machines, you must issue the command on the Gateway Server machine from whose authentication table entries are to be displayed. The command makes no distinction between entries created with the **dfs_login** command and entries created with the **dfsgw add** command. No privileges are required to issue the command.

Note that the **dfsgw list** command provides additional information not available with the **dfsgw query** command, such as the hostname of the NFS client from which each user has DFS access, the principal name of each user

who has DFS access, and the date and time at which each user's DCE credentials expire. See the reference page for the **dfsgw list** command for more information about the command.

Chapter 5. Configuration File and Command Reference

This chapter contains configuration file and command reference information for the NFS/DFS Secure Gateway.

DfsgwLog

Purpose

Log file that contains messages generated by the Gateway Server process of the NFS/DFS Secure Gateway

Description

The **DfsgwLog** file contains messages generated by the Gateway Server (**dfsgwd**) process. The Gateway Server process runs on machines configured as DFS clients to allow users to authenticate to DCE from NFS clients.

If the **DfsgwLog** file does not already exist when the Gateway Server process starts, the process creates the file in the directory named *dcelocal*/**var/dfs/adm**. After the file exists, the process appends messages to it. If the file exists when the Gateway Server process starts, the process moves the current version of the file to the **DfsgwLog.old** file in the same directory (overwriting the current **DfsgwLog.old** file if it exists) before creating a new version to which to append messages.

The process can write different types of output to the file, depending on the actions it performs and any problems it encounters. The file can be viewed with the **bos getlog** command. Because it is an ASCII file, it can also be viewed with the **more** command (or a similar command appropriate to the local operating system), which requires **read** (**r**) permission on the file.

Events are recorded in the log file only at their completion, so the process does not use the file to reconstruct failed operations. However, the contents of the log file can help in evaluating server process failures and other problems.

Related Information

Commands:

bos getlog(8dfs)

dfsgwd(8dfs)

dfsgw

Purpose

Introduction to the **dfsgw** command suite used with the NFS/DFS Secure Gateway

Options

The following options are used with many **dfsgw** commands. They are also described with the commands that use them.

-id *networkID:userID*
Identifies an NFS client and the user whose DCE authentication from that client is to be manipulated. Specify either the network address or the hostname of the NFS client. Specify the user's UNIX user identification number (UID) rather than a username.

-dceid *login_name[:password]*
Specifies the DCE principal name and password of the user for whom to create an entry in the authentication table.

-af *address_family*
Specifies the style of network address to use to identify hosts. By default, the command uses the only address family currently supported, **inet** (Internet).

-help Displays the online help for the command. All other valid options specified with this option are ignored.

Description

The **dfsgw** command suite provides commands to manipulate entries in the local authentication table on a Gateway Server machine. The table contains an entry for each user who has DCE credentials on the Gateway Server machine. Each entry maps the user's UID and the network address of the NFS client for which the user has DCE credentials to the user's Process Activation Group (PAG).

The **dfsgw** command suite includes the following commands:

dfsgw add
Obtains DCE credentials to provide a user with authenticated access to DFS from a specified NFS client. The command adds an entry to the authentication table.

dfsgw delete
Cancels a user's authenticated access to DFS from a specified NFS client by removing the user's entry from the authentication table.

dfsgw list
Displays a list of users who are authenticated to DCE via the Gateway Server machine.

dfsgw query
Determines whether a specific user is authenticated to DCE via the Gateway Server machine. The command determines the user's entry in the authentication table, if it exists.

Commands in the **dfsgw** command suite provide a local administrative interface to the authentication table on a machine configured as a Gateway Server. Because each Gateway Server machine maintains its own authentication table, you must issue **dfsgw** commands on the Gateway Server machine whose authentication table you want to manipulate.

Receiving Help

There are several different ways to receive help about **dfsgw** commands. The following examples summarize the syntax for the different help options:

$ dfsgw help
Displays a list of commands in a command suite.

$ dfsgw help *command*
Displays the syntax for a single command.

$ dfsgw *command* **-help**
Displays the syntax for a single command.

$ dfsgw apropos -topic *string*
Displays a short description of commands that match the specified *string*.

Consult the **dfs_intro(8dfs)** reference page for complete information about the DFS help facilities.

Privilege Required

To use the **add**, **delete**, or **query** command, the issuer must be logged into the Gateway Server machine either as the user whose credentials are to be manipulated or as the local superuser **root**. To use the **list** command, no privileges are required.

All **dfsgw** commands return an exit value of `0` (zero) upon successful completion. Otherwise, they return a nonzero exit value.

Related Information

Commands:

dfsgw_add(8dfs)

dfsgw_apropos(8dfs)

dfsgw_delete(8dfs)

dfsgw_help(8dfs)

dfsgw_list(8dfs)

dfsgw_query(8dfs)

dfs_intro(8dfs)

dfsgw add

Purpose

Adds an entry to the authentication table on the Gateway Server machine

Synopsis

dfsgw add -id *networkID:userID* [**-dceid** *login_name*[:*password*]] [**-sysname** *sysname*] [**-remotehost** *name*] [**-af** *address_family*] **[-help]**

Options

-id *networkID:userID*
: Identifies an NFS client and the user who is to be authenticated to DCE from that client. Specify either the network address or the hostname of the NFS client. Specify the user's UNIX user identification number (UID) rather than a username. The command creates an entry for the user in the local authentication table to provide the user with authenticated access to DFS from the specified NFS client.

-dceid *login_name***[:** *password***]**
: Specifies the DCE principal name and, optionally, the password, of the user for whom an entry is to be added to the authentication table. If you do not specify a principal name and password, the command prompts for them only if you do not already have a valid ticket-granting ticket (TGT) in the current login context. If you omit only your password, the command prompts for your password. The command's interactive prompt provides for secure entry of the password.

-sysname *sysname*
: Specifies the system name for *networkID*. This option defaults to the system name of the Gateway Server machine. The *sysname* argument is a unique name derived from the **uname( )** function that describes the machine architecture and OS type, such as **sparc_sunos57**.

-remotehost *name*
: Specifies the name of the remote host. The default is the hostname of *networkID*.

-af *address_family*
: Specifies the style of network address to use to identify hosts. By default, the command uses the only address family currently supported, **inet** (Internet).

-help Displays the online help for this command. All other valid options specified with this option are ignored.

Description

The **dfsgw add** command authenticates a user to DCE. The command contacts the DCE Security Service to obtain a TGT for the user. To obtain a TGT, a user must have a valid account in the registry database of the DCE cell. The TGT is used to create a valid login context for the user. The login context includes a Process Activation Group (PAG), which DFS stores in the kernel of the Gateway Server machine to identify the user's TGT. The TGT serves as the user's DCE credentials to provide authenticated access to files and directories in the DFS filespace from the specified NFS client.

The **dfsgw add** command adds an entry for the user to the authentication table on the local Gateway Server machine. The entry is a mapping that pairs the user's UID and the network address of the NFS client for which the user has DCE credentials with the user's PAG. Because each Gateway Server machine maintains its own authentication table, you must issue the command on the Gateway Server machine on which an entry is to be added to the authentication table.

The **dfsgw add** command returns an exit value of `0` (zero) if it adds an entry for the user to the authentication table. Otherwise, it returns a nonzero exit value.

DCE credentials obtained with the command are valid for the default ticket lifetime in effect in the registry database of the DCE cell. DCE credentials can be refreshed by issuing the **dfsgw add** command before they expire. In this case, the command automatically associates the user with the DCE principal; it does not have to be supplied. After the credentials expire, they can no longer be used for authenticated access to DFS. You must obtain new credentials by issuing the **dfsgw add** command.

The **dfsgw add** command does not obtain a new TGT if you do not name a principal other than yourself on the command line and you already have a valid TGT in the current login context. If you do not already have an entry in the authentication table for the specified NFS client, the command uses your existing PAG to create a new entry for you. If you already have an entry in the authentication table for the NFS client, the command refreshes your DCE credentials.

Use the **dfsgw delete** command to end an authenticated session by removing an entry from the authentication table.

Privileges Required

The issuer must be logged into the Gateway Server machine either as the user for whom credentials are to be created or as the local superuser **root**.

Output

The **dfsgw add** command displays the following prompts to request a DCE principal and password:

```
Enter Principal Name:  principal
Enter Password:  password
```

where *principal* is the name of the user to be authenticated to DCE, and *password* is the password of the named user; you supply both of these values. The command prompts for the *principal* name only if you do not specify a principal name with the **-dceid** option and you do not already have a valid TGT. The command prompts for the *password* only if you do not specify a password with the **-dceid** option and if either of the following is true:

- You name a user other than yourself with the **-dceid** option
- You do not already have a valid TGT

If it succeeds in creating the entry in the authentication table, the command displays the following:

```
Mapping added successfully, PAG is PAG
```

where *PAG* identifies the PAG created with the command.

Examples

The following command creates an entry in the authentication table to grant authenticated access to DFS to the user named **ludwig**. The user, whose UID is **7439**, is requesting access from the NFS client that has network address **15.27.32.40**. The user provides the principal name with the **-dceid** option but omits the password; the command prompts for the user's password, which the user specifies as **beethoven** in the example.

```
$ dfsgw add -id 15.27.32.40:7439 -dceid ludwig
Enter Password: beethoven
Mapping added successfully, PAG is 41ffffe4
```

Related Information

Commands:

dfsgw_delete(8dfs)

dfsgw_list(8dfs)

dfsgw_query(8dfs)

dfsgw apropos

Purpose

Displays the help entry for each **dfsgw** command that contains a specified string

Synopsis

dfsgw apropos -topic *string* [**-help**]

Options

-topic *string*
: Specifies the keyword string for which to search. If it is more than a single word, surround the string with double quotes (″ ″) or other delimiters. Type all strings in lowercase letters.

-help Displays the online help for this command. All other valid options specified with this option are ignored.

Description

The **dfsgw apropos** command displays the first line of the help entry for any **dfsgw** command that contains the string specified by the **-topic** option in its name or short description.

To display the syntax for a command, use the **dfsgw help** command.

Privilege Required

No privileges are required.

Output

The first line of an online help entry for a command names the command and briefly describes its function. This command displays the first line for any **dfsgw** command where the string specified by the **-topic** option is part of the command name or the first line.

Examples

The following command lists all **dfsgw** commands that have the word **entry** in their names or short descriptions:

```
$ dfsgw apropos entry
add: add an entry to the AT
delete: delete an entry from the AT
```

Related Information

Commands:

dfsgw help(8dfs)

dfsgw delete

Purpose

Removes an entry from the authentication table on the Gateway Server machine

Synopsis

dfsgw delete -id *networkID:userID* [**-af** *address_family*] [**-help**]

Options

-id *networkID:userID*
: Identifies an NFS client and the user whose authentication to DCE from that client is to be canceled. Specify either the network address or the hostname of the NFS client. Specify the user's UNIX user identification number (UID) rather than the username. The command removes the user's entry for the specified NFS client from the local authentication table.

-af *address_family*
: Specifies the style of network address to use to identify hosts. By default, the command uses the only address family currently supported, **inet** (Internet).

-help
: Displays the online help for this command. All other valid options specified with this option are ignored.

Description

The **dfsgw delete** command cancels a user's authenticated access to DFS. The command removes the entry for the specified user and NFS client from the authentication table on the Gateway Server machine.

Because each Gateway Server machine maintains its own authentication table, you must issue the command on the Gateway Server machine from which to remove an entry from the authentication table. The command has no effect on entries the user has in the authentication table for other NFS clients, and it has no effect on entries in the authentication tables on other Gateway Server machines.

The **dfsgw delete** command returns an exit value of `0` (zero) if it removes the entry for the specified user from the authentication table. Otherwise, it returns a nonzero exit value.

To obtain DCE credentials and create an entry in the authentication table, use the **dfsgw add** command.

Privilege Required

The issuer must be logged into the Gateway Server machine either as the user whose entry is to be removed from the authentication table or as the local superuser **root**.

Examples

The following command deletes the entry from the authentication table that grants authenticated access to the user named **ludwig** from the NFS client that has network address **15.27.32.40**. The command is issued by the user **ludwig**, who has UID **7439**.

```
$ dfsgw del -id 15.27.32.40:7439
```

Related Information

Commands:

dfsgw_add(8dfs)

dfsgw_list(8dfs)

dfsgw_query(8dfs)

dfsgw help

Purpose

Shows syntax of specified **dfsgw** commands or lists functional descriptions of all **dfsgw** commands

Synopsis

dfsgw help [**-topic** *string*] [**-help**]

Options

-topic *string*
: Specifies each command whose syntax is to be displayed. Provide only the second part of the command name (for example, **list**, not **dfsgw list**). If this option is omitted, the output provides short descriptions of all **dfsgw** commands.

-help
: Displays the online help for this command. All other valid options specified with this option are ignored.

Description

The **dfsgw help** command displays the first line (name and short description) of the online help entry for every **dfsgw** command if the **-topic** option is not provided. For each command name specified with the **-topic** option, the output lists the entire help entry.

Use the **dfsgw apropos** command to show each help entry that contains a specified string.

Privilege Required

No privileges are required.

Output

The online help entry for each **dfsgw** command consists of the following two lines:

- The first line names the command and briefly describes its function.
- The second line, which begins with `Usage:`, lists the command options in the prescribed order.

Examples

The following command displays the online help entry for the **dfsgw list** command:

```
$ dfsgw help list
```

```
dfsgw list: list all entries in the AT
Usage: dfsgw list [-help]
```

Related Information

Commands:

dfsgw apropos(8dfs)

dfsgw list

Purpose

Lists all entries in the authentication table on the Gateway Server machine

Synopsis

dfsgw list [**-help**]

Options

-help Displays help information for this command.

Description

The **dfsgw list** command lists all entries from the local authentication table, which indicate which users on NFS clients have DCE credentials. Because each Gateway Server machine maintains its own authentication table, you must issue the command on the Gateway Server machine that houses the authentication table from which entries are to be displayed.

Use the **dfsgw query** command to see the entry in the authentication table for a specific user. Note that the **dfsgw list** command provides some additional information not displayed by the **dfsgw query** command. For example, it displays the hostname of the NFS client for which the DCE credentials are granted, the principal name of the user to whom the credentials are granted, the date and time at which the credentials expire, and the system name and remote hostname used for the client.

The **dfsgw list** command returns an exit value of `0` (zero) if it succeeds in listing the entries from the authentication table. Otherwise, it returns a nonzero exit value.

Privileges Required

No privileges are required.

Output

The **dfsgw list** command displays the following output for each entry in the authentication table:

```
Mapping:  hostname : principal => PAG
Expires at date/time
@host=remotehost @sys=sysname
```

where

hostname
Names the NFS client for which the entry grants authenticated access to DFS

principal
Displays the principal name of the user to whom the entry grants authenticated access

PAG Identifies the Process Activation Group (PAG) that exists for the *hostname/principal* pair

date/time
Specifies the date and time at which the DCE credentials identified by the PAG expire

remotehost
Identifies the remote hostname used for the *hostname/principal* pair

sysname
Identifies the system name used for the *hostname/principal* pair

The **dfsgw list** command displays the following output if the authentication table contains no entries:

```
No mappings exist
```

Examples

The following command displays the current entries from the authentication table on the local Gateway Server machine. The first entry grants secure access to DFS to the user **ludwig** from the NFS client named **nfs1.abc.com**. The PAG associated with the user is **41ffffe4**; the user's DCE credentials expire at 5:59 a.m. on 17 Nov 1999.

```
dfsgw list
Mapping: nfs1.abc.com:ludwig => 41ffffe4
Expires at Wed Nov 17 05:59:18 1999
(@host=host1.xyz.com @sys=sparc_sunos57)
Mapping: nfs2.abc.com:frost => 41ffffa3
Expires at Wed Nov 17 08:36:23 1999
(@host=host2.xyz.com @sys=sparc_sunos57)
Mapping: nfs2.abc.com:wvh => 41ffffbe
Expires at Thu Nov 17 00:51:21 1999
(@host=host3.xyz.com @sys=sparc_sunos57)
.
.
.
```

Related Information

Commands:

dfsgw_add(8dfs)

dfsgw_delete(8dfs)

dfsgw_query(8dfs)

dfsgw query

Purpose

Queries the authentication table on the Gateway Server machine

Synopsis

dfsgw query -id *networkID:userID* [**-af** *address_family*] [**-help**]

Options

-id *networkID:userID*
: Identifies an NFS client and the user whose authentication from the client is to be determined. Specify either the network address or the hostname of the NFS client. Specify the user's UNIX user identification number (UID) rather than the username. The command searches the local authentication table to determine whether the user has an entry for the specified NFS client.

-af *address_family*
: Specifies the style of network address to use to identify hosts. By default, the command uses the only address family currently supported, **inet** (Internet).

-help
: Displays the online help for this command. All other valid options specified with this option are ignored.

Description

The **dfsgw query** command checks the local authentication table to determine whether the user has an entry for the NFS client. Because each Gateway Server machine maintains its own authentication table, you must issue the command on the Gateway Server machine that houses the authentication table to be queried. The command determines only whether the user has an entry for the specified client; the command does not report whether the user has entries for any other clients.

Use the **dfsgw list** command to see all entries in the authentication table. The **dfsgw list** command provides some additional information not displayed by the **dfsgw query** command. The **dfsgw query** command is useful for inclusion in scripts that determine only whether a user has authenticated access to DFS from an NFS client.

The **dfsgw query** command returns an exit value of `0` (zero) if it finds an entry for the specified user in the authentication table. Otherwise, it returns a nonzero exit value.

Privilege Required

The issuer must be logged into the Gateway Server machine either as the user whose entry in the authentication table is to be examined or as the local superuser **root**.

Output

The **dfsgw query** command displays the following line of output if the specified user has an entry for the specified NFS client in the authentication table:

```
Mapping found, PAG is PAG
```

where *PAG* identifies the Process Activation Group (PAG) that exists for the user. If the user does not have an entry for the NFS client in the authentication table, the **dfsgw query** command displays the following line of output instead:

```
No mapping found
```

Examples

The following command determines whether the authentication table on the local Gateway Server machine includes an entry for the user named **ludwig** from the NFS client that has network address **15.27.32.40**. The user **ludwig** has UID **7439**. The command reports that **ludwig** has an entry in the table; the PAG associated with the user is **41ffffe4**.

```
$ dfsgw query -id 15.27.32.40:7439
Mapping found, PAG is 41ffffe4
```

Related Information

Commands:

dfsgw_add(8dfs)

dfsgw_delete(8dfs)

dfsgw_list(8dfs)

dfsgwd

Purpose

Initializes the Gateway Server process for the NFS/DFS Secure Gateway

Synopsis

dfsgwd [**-service** *service_number*] [**-sysname** *sysname*] [**-nodomains**] [**-file** *log_file*] [**-verbose**] [**-help**]

Options

-service *service_number*
: Specifies the port number to be used to communicate with the **dfsgwd** process on the Gateway Server machine. By default, the process uses port number **438**, the port number defined for the Gateway Server process in the **/etc/services** file or Network Information Services (NIS) services map file.

-sysname *sysname*
: Specifies the system name for this Gateway Server. The **dfsgwd** process can handle NFS clients that do not recognize the **@sys** and **@host** variables, using a system name of **unknown**. (See the *IBM DFS for AIX and Solaris Administration Guide* for more information on the **@sys** and **@host** variables.) This name can be set by starting the **dfsgwd** process with the **-sysname** option. The *sysname* argument is a unique name derived from the **uname( )** function that describes the machine architecture and OS type, such as **sparc_sunos57**.

-nodomains
: Uses the base hostname (without the domain portion) for the **@host** variable.

-file *log_file*
: Specifies the full pathname of the log file in which the **dfsgwd** process records information about the operations it performs. By default, the **dfsgwd** process writes output to the log file named *dcelocal***/var/dfs/adm/DfsgwLog**.

-verbose
: Directs the process to write a message of the following form to the indicated log file each time an entry is added to the authentication table:

```
INFO:  Adding ticket for "username"
```

where *username* is the name of the user for whom the entry is added.

-help Displays the online help for this command. All other valid options specified with this option are ignored.

Description

The **dfsgwd** command initializes the Gateway Server process. The **dfsgwd** process runs on machines configured as DFS clients to enable remote authentication via the **dfs_login** command. The **dfsgwd** process works with the **dfs_login** command to obtain DCE credentials for users of NFS clients. The DCE credentials provide users with authenticated access to data in DFS.

The Gateway Server process manipulates mappings for authenticated users in the authentication table on the Gateway Server machine. Each mapping records the following information for an authenticated user:

- The user's UNIX user identification number (UID)
- The network address of the NFS client from which the user has authenticated access to DFS
- The PAG that stores the user's DCE ticket-granting ticket (TGT)

The **dfs_login** and **dfs_logout** commands provide a remote mechanism for creating and deleting entries in the authentication table on a Gateway Server machine. Commands in the **dfsgw** command suite provide a local administrative interface to the authentication table on a machine configured as a Gateway Server.

The Gateway Server process recognizes the **@sys** and **@host** variables on the NFS client system. This allows the Gateway Server to resolve pathnames to binaries and other system-dependent files correctly, based on the user's login system name and system type.

The binary file for the **dfsgwd** process resides in *dcelocal*/**bin**. The process is normally run on a DFS client that is exporting a mount point for **/...**, the root of the DCE namespace, via NFS. The process runs as the DCE principal **hosts/** *hostname*/**dfsgw-server**.

The **dfsgwd** process is usually started and controlled by the Basic OverSeer (BOS) Server (**bosserver**) process. The BOS Server restarts each process it monitors whenever the system is restarted. If the **dfsgwd** process is not controlled by the BOS Server, the **dfsgwd** process runs in the foreground by default.

The **dfsgwd** process writes output about the operations it performs to a log file, by default, named *dcelocal*/**var/dfs/adm/DfsgwLog**. You can use the **-file** option to name a different log file. If the **dfsgwd** process is controlled by the BOS Server, you can use the **bos getlog** command to read the log file.

Privileges Required

The issuer must be the local superuser **root** on the local machine.

Files

dcelocal/**var/dfs/adm/DfsgwLog**
: The default log file for the **dfsgwd** process. You can use the **-file** option to specify a different pathname for the log file.

Related Information

Commands:

bos getlog(8dfs)

bosserver(8dfs)

dfsgw(8dfs)

Files:

DfsgwLog(4dfs)

Index

Special Characters

A

B

C

D

G

K

L

N

R

S

Notices

First Edition (April 2000)

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
ATTN: Software Licensing
11 Stanwix Street
Pittsburgh, PA 15222-1312
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices show are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples may include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

The following terms are trademarks of International Business Machine Corporation in the United States, other countries, or both:

AFS
AIX
AS/400
CICS
CICS OS/2
CICS/400
CICS/6000
CICS/ESA
CICS/MVS
CICS/VSE
CICSPlex
DB2
DCE Encina Lightweight Client
DFS
Encina
IBM
IMS
MQSeries
MVS/ESA
OS/2
OS/390
OS/400
PowerPC
RISC System/6000
RS/6000
S/390
Transarc
TXSeries
VSE/ESA
VTAM
VisualAge
WebSphere

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries or both.

Sun, SunLink, Solaris, SunOS, Java, all Java-based trademarks and logos, NFS, and Sun Microsystems are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Readers' Comments — We'd Like to Hear from You

DFS for Solaris
NFS/DFS Secure Gateway Guide and Reference
Version 3.1

Publication No. GC09-3993-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
GC09-3993-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
ATTN: File Systems Documentation Group
11 Stanwix Street
Pittsburgh, PA
15222-1312

Fold and Tape **Please do not staple** Fold and Tape

GC09-3993-00

Cut or Fold
Along Line

Program Number:

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC09-3993-00

Spine information:

DFS for Solaris

NFS/DFS Secure Gateway Guide and Reference

Version 3.1

GC09-3993-00